REMARKS

Claims 1-9, 12-17, 19-21, 23-41, and 45-47 are currently pending in the subject application and are presently under consideration. Claims 1-2, 8, 12, 16-17, 21, 26, 30-31, 34, 39, and 41 have been amended as shown on pages 2 to 9 of the Reply. Applicants' representative appreciates courtesies extended by the Examiner in the telephonic interview for the subject application conducted on October 21, 2008, where no agreement was reached as to the subject claims. Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1-9, 12-17, 19-21, 23-41, and 45-47 Under 35 U.S.C. §102(b)

Claims 1-9, 12-17, 19-21, 23-41, and 45-47 stand rejected under 35 U.S.C. §102(b) as being anticipated by Swiler, *et al.* (US 7,013,395). It is respectfully requested that this rejection be withdrawn for at least the following reasons. Swiler, *et al.* fails to disclose or suggest each and every element recited in the subject claims.

> A single prior art reference anticipates a patent claim only if it expressly or inherently describes ***each and every limitation set forth in the patent claim***. *Trintec Industries, Inc. v. Top-U.S.A. Corp.,* 295 F.3d 1292, 63 USPQ2d 1597 (Fed. Cir. 2002); *See Verdegaal Bros. v. Union Oil Co. of California,* 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

The subject matter as claimed generally relates to generating a set of security guidelines, security data, and/or security components. In particular, input can be received in the form of an abstract description or model of a factory, wherein the factory description includes one or more PLC-based industrial controllers to be protected, and associated network pathways to access the controllers. The generated security data can include a set of recommended security components, related interconnection topology, connection configurations, application procedures, security policies, rules, user procedures, and/or user practices related to the industrial controllers. To this end, claim 1 as amended recites, in part, ***an interface component to generate a description of one or more programmable logic controller (PLC)-based industrial controllers***. Swiler *et al.* fails to disclose such claimed aspects.

Swiler, *et al.* generally relates to a tool that analyzes computer systems for security attributes related thereto. (*See*, Abstract). In particular, Swiler, *et al.* appears to contemplate generating an attack graph based at least in part on inputs including attack templates, configuration files, and attacker profiles. Swiler, *et al.* generally contemplates security analysis for computers, such as "workstations, servers, or routers." (*See e.g.*, column 4, lines 48-52). However, Swiler, *et al.* fails to disclose or suggest operability with industrial controllers, much less ***an interface component to generate a description of one or more programmable logic controller (PLC)-based industrial controllers***, as recited in claim 1.

On the contrary, Swiler, *et al.* deals with computer systems, as evidenced by explicit disclosures relating to computers, workstations, servers, routers, *etc.* Applicants' claims are not so limited and recite operability with PLC-based industrial controllers. Swiler, *et al.* is completely silent regarding this aspect. In the sections cited by the Examiner, Swiler, *et al.* appears to disclose operability in different computing environments, including governmental, commercial, and civilian operations. However, Swiler, *et al.* merely refers to computers in these environments, and not ***one or more programmable logic controller (PLC)-based industrial controllers***, as recited in claim 1. PLC-based industrial controllers can utilize different protocols and have varying input and outputs as compared to computers, in one example. Accordingly, PLC-based industrial controllers can have different security needs, and indeed, implementation details than computers. Thus, recitation of a system operable with computers is not indicative of one operable with PLC-based industrial controllers as in applicants' claims. Thus, Swiler, *et al.* fails to disclose or suggest each and every element recited in claim 1.

Moreover, claim 12, as amended, recites similar aspects, namely *inputting at least one model related to* ***one or more programmable logic controller (PLC)-based industrial controllers*** *and* ***monitoring access to the PLC-based industrial controllers to learn at least one access pattern***. As Swiler, *et al.* fails to disclose or suggest industrial controller, much less PLC-based industrial controller operability, it also cannot be said to disclose monitoring the controllers as recited in claim 12. Thus, Swiler, *et al.* additionally fails to disclose or suggest all aspects of claim 12. Claim 16 recites similar aspects as well, *namely means* ***for receiving abstract descriptions of one or more programmable logic controller (PLC)-based industrial controllers*** and *means for* ***learning at least one access pattern for accessing the PLC-based industrial controllers***. Again, Swiler, *et al.* cannot be said to recite receiving such a description

or learning an access pattern as it does not disclose or suggest operability with PLC-based industrial controllers. Thus, Swiler, *et al.* does not disclose or suggest all aspects of claim 16.

In addition, claim 17 as amended recites similar aspects, namely ***a scanner component to automatically interrogate a programmable logic controller (PLC)-based industrial automation device at periodic intervals for security related data***. Swiler, *et al.* does not perform such interrogation as it does not communicate with such controllers. Thus, Swiler, *et al.* does not disclose or suggest all aspects of claim 17. Further, claim 26 as amended recites ***scanning one or more programmable logic controller (PLC)-based industrial automation devices for potential security violations at periodic intervals, wherein identity information about end devices that relates to hacker entry is gained***. Swiler, *et al.* is silent regarding these aspects at least since it does not disclose or suggest scanning PLC-based industrial automation devices, as shown.

Additionally, claim 30 as amended recites, in part, *means for* ***scanning one or more programmable logic controller (PLC)-based industrial automation devices*** *for potential security violations* and *means for* ***performing at least one of security assessments, security compliance checks, and security vulnerability scanning of the PLC-based industrial automation*** *devices to mitigate the security violations*. As shown, Swiler, *et al.* fails to disclose or suggest such aspects. Also, claim 31, as amended, recites similar aspects of ***a learning component to monitor and learn industrial automation activities on one or more programmable logic controllers (PLC) during a training period***. Swiler, *et al.*, not contemplating applicability to industrial controllers (much less PLC-based controllers) cannot be said to disclose or suggest such aspects. Furthermore, claim 39 recites, in part, ***monitoring a network of programmable logic controller (PLC)-based industrial controllers for a predetermined time***. Swiler, *et al.* does not disclose or suggest such aspects, as shown. Moreover, claim 41 recites similar aspects of *means for* ***learning access patterns to at least one programmable logic controller (PLC)-based industrial automation device from the network***. Swiler, *et al.* does not contemplate such aspects as shown.

In view of the foregoing, it is readily apparent that Swiler, *et al.* fails to disclose or suggest each and every element recited in claims 1, 12, 16, 17, 26, 30, 31, 39, and 41. Accordingly, it is respectfully requested that rejection of these claims, as well as claims 2-9, 13-15, 19-21, 23-25, 27-29, 32-38, 40, and 45-47, which depend therefrom, be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [ALBRP303USC].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/David Matthew Noonan/
David Matthew Noonan
Reg. No. 59,451

AMIN, TUROCY & CALVIN, LLP
57TH Floor, Key Tower
127 Public Square
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731